

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-184992

(43)Date of publication of application : 09.07.1999

(51)Int.Cl.

G06K 17/00

G06T 7/00

G06K 19/10

G06K 19/07

(21)Application number : 09-354268

(71)Applicant : CASIO COMPUT CO LTD

(22)Date of filing : 24.12.1997

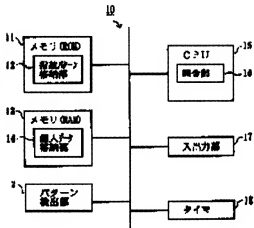
(72)Inventor : YAMAKITA TORU

(54) IC CARD AND DEVICE FOR INSERTING THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To attain improvement in security by judging whether an IC card is used by an authorized user or not while using a fingerprint pattern.

SOLUTION: A memory 11 is provided with a fingerprint pattern storage part 12 as a ROM area for storing the fingerprint pattern of a prescribed finger of the card user. A pattern detecting part 2 detects the rugged surface of an object pressed onto its surface. A collation part 16 of a CPU 15 is provided by executing one part of a program and collates the fingerprint pattern stored in the fingerprint pattern storage part 12 with the fingerprint pattern of the card user read by the pattern detecting part 2. Thus, the IC card itself judges whether a person to use the IC card is the authorized user or not and reports the judged result to a main body device. When the IC card is used by a person, who is not an authorized user (illegally used), the main body device inhibits processing based on that IC card.



LEGAL STATUS

[Date of request for examination]

09.12.2002

[Date of sending the examiner's decision of rejection]

31.05.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

特開平11-184992

(43)公開日 平成11年(1999)7月9日

(51)Int.Cl. ⁸ G 0 6 K 17/00 G 0 6 T 7/00 G 0 6 K 19/10 19/07	識別記号	F I G 0 6 K 17/00 V B G 0 6 F 15/02 4 6 0 G 0 6 K 19/00 S J
		審査請求 未請求 請求項の数7 O L (全 15 頁)
(21)出願番号	(71)出願人 000001443 カシオ計算機株式会社 東京都渋谷区本町1丁目6番2号	
(22)出願日	平成9年(1997)12月24日	
		(72)発明者 山北 徹 東京都羽村市柴町3丁目2番1号 カシオ 計算機株式会社羽村技術センター内
		(74)代理人 弁理士 阪本 紀康

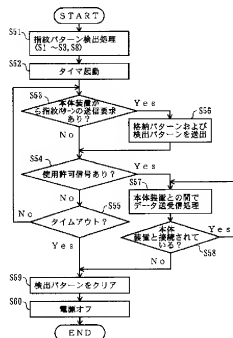
(54)【発明の名称】 ICカードおよびICカードが挿入される装置

(57)【要約】

【課題】 使用者の負担を小さくしながら高いセキュリティが得られるICカードおよびそのICカードが挿入される装置を提供する。

【解決手段】 ICカードは、使用者の指紋パターンを検出し、その検出した指紋パターンおよび予め格納してある指紋パターンを本体装置に送出する。本体装置は、これら2つの指紋パターンを照合し、一致した場合にはICカードに対して使用許可信号を送信する。ICカードは、使用許可信号を受信すると、本体装置との間でデータの送受信を行う。

第1の実施例のICカードの処理のフローチャート



【特許請求の範囲】

【請求項1】 物体の表面のパターンを検出する検出手段と、

指紋パターンを格納する格納手段と、
上記検出手段により検出された指紋パターンと上記格納手段に格納されている指紋パターンとを照合し、その照合結果を出力する照合手段と、を有し、
上記照合手段が出力する照合結果に基づいて処理を許可するか否かを判断する装置に挿入されるICカード。

【請求項2】 上記照合手段は、上記照合結果を所定期間出力する請求項1に記載のICカード。

【請求項3】 物体の表面のパターンを検出する検出手段と、

指紋パターンを格納する格納手段と、
上記検出手段により検出された指紋パターンおよび上記格納手段に格納されている指紋パターンを出力する出力手段と、を有し、
上記出力手段が出力する各指紋パターンを照合して処理を許可するか否かを判断する装置に挿入されるICカード。

【請求項4】 ICカードが挿入される装置であって、
上記ICカードに予め格納されている指紋パターンとそのICカードが検出した指紋パターンとの照合結果として、
それら2つの指紋パターンが互いに一致している旨の通知をそのICカードから受信した際に、そのICカードに基づく処理を許可する装置。

【請求項5】 上記ICカードが、照合結果として、上記2つの指紋パターン間の類似度を複数段階で評価した結果を出力した場合、
類似度の段階に応じて、

そのICカードに基づく処理を許可し、
もしくは、使用者にパスワードを要求してその要求に対して正規のパスワードが入力された場合にそのICカードに基づく処理を許可し、
もしくは、そのICカードに基づく処理を禁止する、
請求項4に記載の装置。

【請求項6】 ICカードが挿入される装置であって、
上記ICカードに予め格納されている指紋パターンおよびそのICカードが検出した指紋パターンをそのICカードから受信する受信手段と、
上記2つの指紋パターンを照合し、それらが互いに一致していた場合にそのICカードに基づく処理を許可する照合手段と、
を有する装置。

【請求項7】 上記照合手段は、上記2つの指紋パターン間の類似度を複数段階で評価し、類似度の段階に応じて、

そのICカードに基づく処理を許可し、
もしくは、使用者にパスワードを要求してその要求に対して正規のパスワードが入力された場合にそのICカード

に基づく処理を許可し、
もしくは、そのICカードに基づく処理を禁止する、
請求項6に記載の装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ICカード、および挿入されたICカードとの間でデータを送信または受信する装置に係わる。

【0002】

【従来の技術】従来から、使用者の身分証明（ID）としての機能が電子的に組み込まれたカードが広く普及している。たとえば、銀行等の口座にアクセスするための、いわゆるキャッシュカードやクレジットカード、あるいはドアのロックを解除したり、各種装置を起動するためのIDカードなどである。これらのカードには、通常、そのカードの使用者を識別する情報が書き込まれた磁気フィルム等が貼り付けられている。そして、使用時には、そのカードが挿入された装置がその識別情報を読み取り、アクセス等の処理を許可するか否かを判断する。

【0003】ところが、上述のような単純な方式だと、カードを紛失した場合などには、それを拾った他人が不正にそのカードを使用できることになる。そこで、キャッシュカード等においては、上述のような磁気フィルム等に書き込まれた識別情報と共に、暗証番号（パスワード）が併用されることが一般的である。例えば、キャッシュカードが挿入されると、ユーザーに暗証番号を要求し、その要求に対して予め登録されている正規の暗証番号が投入されたときのみアクセスを許可するようなシステムは広く実施されている。

【0004】また、近年、上述のようなカードにインテリジェントな機能を持たせるために集積回路を組み込んだカード型の機器（通常、ICカードと呼ばれることが多いので、以下、そのように呼ぶことにする）の研究・開発が盛んである。ICカードは、将来、電子マネーや電子財布の分野においてその中心的な役割を担うことが予想されているので、特に、他人の不正使用を防ぐために高いセキュリティを確保することが必須の要件となっている。

【0005】

【発明が解決しようとする課題】現在、他人による各種カード類（ICカードを含む）の不正使用を防ぐ手法としては、暗証番号（パスワード）が最も一般的である。ところが、この場合、各カード使用者は、暗証番号を覚えておく必要があり、特に所持するカードの枚数が多いとその負担が大きくなっていた。また、暗証番号は、流出してしまう恐れがあった。

【0006】本発明の課題は、上述の問題を解決することであり、使用者の負担を小さくしながら高いセキュリティが得られるICカードおよびそのICカードが挿入

される装置を提供することである。

【0007】

【課題を解決するための手段】本発明のICカードは、物体の表面のパターンを検出する検出手段と、指紋パターンを格納する格納手段と、上記検出手段により検出された指紋パターンと上記格納手段に格納されている指紋パターンとを照合し、その照合結果を出力する照合手段と、を有する。

【0008】上記ICカードが挿入される装置は、そのICカードに予め格納されている指紋パターンとそのICカードが検出した指紋パターンとの照合結果としてそれら2つの指紋パターンが互いに一致している旨の通知をそのICカードから受信した際に、そのICカードに基づく処理を許可する構成である。

【0009】上記構成によれば、格納手段に格納されている指紋パターンを持つ者以外の者がこのICカードを使用すると、照合手段による照合結果は不一致となる。したがって、上記ICカードが挿入される装置は、そのICカードに基づく処理を禁止する。このようにして、指紋パターンにより不正使用を防ぐ。

【0010】本発明の他の形態のICカードは、物体の表面のパターンを検出する検出手段と、指紋パターンを格納する格納手段と、上記検出手段により検出された指紋パターンおよび上記格納手段に格納されている指紋パターンを出力する出力手段とを有する。

【0011】上記他の形態のICカードが挿入される装置は、そのICカードに予め格納されている指紋パターンおよびそのICカードが検出した指紋パターンをそのICカードから受信する受信手段と、上記2つの指紋パターンを照合し、それらが互いに一致していた場合にそのICカードに基づく処理を許可する照合手段と、を有する構成である。この形態の作用は、上述した作用と同じである。

【0012】

【発明の実施の形態】以下、本発明の実施形態について図面を参照しながら説明する。図1(a)および(b)は、本実施形態のICカードの外観図である。ICカード1は、たとえば、銀行口座へのアクセス、商品購入時の支払い、ドアロックの解除、あるいは各種装置の起動などに際して使用されるカード型の機器である。ICカード1は、その表面の一部に、パターン検出部2が設けられている。パターン検出部2は、そこに接触された物体の表面のパターン（凹凸パターン等）を検出する機能を有し、本実施形態では、カード使用者の指紋パターンを読み取るために使用される。

【0013】カード使用者は、ICカード1を使用する際には、まず、スイッチをオンにした後、予め決められている指をパターン検出部2に押圧する。図1(a)に示す例では、右手の人差し指をパターン検出部2に押圧する例を示している。所定の指をパターン検出部2に押

圧するときには、指紋パターンが確実に検出されるように、親指を使ってICカード1を挟み付けるようにすることが望ましい（図1(b)参照）。

【0014】ICカード1は、その使用者の所定の指（図1に示す実施例では、右手の人差し指）の指紋パターンが予め格納されている。そして、後述する第1および第2の実施例では、ICカード1は、その予め格納されている指紋パターンとパターン検出部2により検出された指紋パターンとを照合し、その照合結果を出力する。また、第3の実施例では、ICカード1は、そのカードが挿入される本体装置に対して、上記予め格納されている指紋パターンおよびパターン検出部2により検出された指紋パターンを出力し、その本体装置がそれらの指紋パターンを照合する。そして、本体装置は、各実施例において、上記2つの指紋パターンが一致したときに、ICカード1に基づく処理（ICカード1を用いたアクセスを含む）を許可し、以降、その間でデータを送受信する。

第1の実施例

第1の実施例は、ICカードに指紋照合機能を持たせた構成である。

【0015】図2は、第1（および第2）の実施例のICカード10の構成図である。メモリ11は、ROM領域であり、カード使用者の所定の指の指紋パターンを格納するための指紋パターン格納部12を含む。この指紋パターンは、たとえば、カードの発行時に格納される。メモリ11には、後述するフローチャートの処理を記述したプログラム等も格納されている。メモリ13は、RAM領域であり、上記プログラムを実行する際に使用される領域の他、カード使用者の個人情報を格納する個人データ格納部14が設けられている。個人データ格納部14は、たとえば、このICカード10が電子マネーシステムにおける電子財布であったとすると、「財布中の金額」に相当する情報などを格納する。なお、個人データ格納部14は、不揮発性メモリ領域に設けられる。

【0016】パターン検出部2は、その表面に押圧された物体の表面の凹凸を検出する装置であり、微細化技術の進歩によりICカードに組み込むことができる程度に薄く形成されている。パターン検出部2は、たとえば、光源および2次元フォトセンサを含み、その2次元フォトセンサを構成する多数の受光素子がそれぞれ検出する受光レベルに対応する電流値または電圧値をシリアル形式またはパラレル形式で出力する。なお、本発明の出願人は、先に、十分に薄型でありながら高い精度で物体の表面の凹凸パターンを検出することができる読取装置について特許出願をしている（特願平9-222018号）。

【0017】CPU15は、メモリ11に格納されているプログラムを実行する。CPU15は、照合部16を備える。照合部16は、上記プログラムの一部を実行す

ることにより実現され、指紋パターン格納部12に格納されている指紋パターンとパターン検出部2により読み取られたカード使用者の指紋パターンとを照合する。入出力部17は、このICカード10が挿入される本体装置2の間でデータを送受信する。タイマ18は、CPU15により起動され、所定時間が経過するとCPU15に割込信号を送出する。

【0018】図3は、第1（および第2）の実施例の本体装置20の構成図である。この本体装置20には、図2に示したICカード10が挿入される。ICカード10は、カード挿入部21に挿入される。カード挿入部21は、ICカード10とのインタフェースをとるためのI/F部22を備える。CPU23は、メモリ24に格納されているプログラムを実行することにより、ICカード10とのデータの授受、また、必要に応じて不図示の外部装置（ホストコンピュータなど）とのデータの授受を制御する。メモリ24は、後述するフローチャートの処理を始め、この本体装置20の各ソフトウェア処理を記述したプログラムおよびこの本体装置20が使用する各種データを格納する。なお、ここでは、カード挿入部21、CPU23およびメモリ24が1つの装置の中に設けられているように記載しているが、これらを互いに異なる場所に設け、通信回線等を用いた互いに接続する構成であってもよい。

【0019】図4および図5は、第1の実施例におけるICカードの処理のフローチャートである。この処理は、ICカードの電源をオンにしたことをトリガとして実行される。

【0020】ステップS1では、電源がオンにされたときから一定時間内にパターン検出部2に入力があったか否かを調べる。この処理は、たとえば、パターン検出部2の出力が変化したか否かを調べるものである。パターン検出部2に入力があった場合には、ユーザが所望の指の指先（指紋が形成されている部分）をパターン検出部5に押圧したものと見なし、ステップS2へ進み、一方、入力が無かった場合には、ステップS8においてICカードの電源をオフにする。

【0021】ステップS2では、指紋パターンを検出する。すなわち、パターン検出部5の出力を取り込む。この指紋パターンは、たとえば、メモリ13の所定の領域に保持される。ステップS3では、指紋パターンを適切に検出できたか否かを判断する。すなわち、ユーザの指がパターン検出部2に一定時間以上固定されなかった場合や、押圧が弱く接触面積が小さかった場合などには、指紋パターンを再生できないので、このステップで指紋パターンを適切に検出できたか否かを判断している。指紋パターンを適切に検出できた場合には、ステップS4へ進み、検出できなかった場合にはステップS1へ戻る。

【0022】ステップS4では、指紋パターン格納部1

2に格納されている指紋パターンとパターン検出部2により検出された指紋パターンとを照合する。この処理は、例えば、上記2つの指紋パターンの類似度を数値化する手順を含む。

【0023】ステップS5では、上記ステップS4により得られた類似度を表す値が、予め設定してある閾値を越えるか否かに従って「一致／不一致」を判断する。上記2つの指紋パターンが互いに一致していた場合には、ステップS6において、OK信号を出力する。この処理は、例えば、このICカードが挿入される本体装置20のI/F部22と接続する端子の中の所定の1つを「L」レベルから「H」レベルに切り換えるものである。ステップS7では、タイマ18を起動する。

【0024】ステップS11およびS12では、使用許可信号を受信しているか否かを調べる。なお、この使用許可信号は、後述説明するが、図4に示した本体装置20により生成される信号であり、本体装置20がそこに挿入されたICカードに基づく処理を許可すると判断した際に本体装置20によって出力される。ここで、タイマ18に設定されている所定の時間が経過する前に使用許可信号を受信した場合には、ステップS16およびS17において、本体装置20の間でデータを送受信する処理を実行する。この処理は、ICカードが本体装置20と接続されている間は継続される。

【0025】本体装置20がこのICカードを排出するなどして本体装置20との接続が終了すると、ステップS13へ進んでOK信号をリセットする。すなわち、OK信号の送出手を停止する。続いて、ステップS14では、ステップS2においてパターン検出部2により検出した指紋パターンをクリアする。そして、ステップS15において、このICカードの電源をオフにする。

【0026】一方、ステップS11およびS12において、タイマ18に設定されている所定の時間が経過するまでに使用許可信号を受信できなかった場合、すなわち、タイマ18がタイムアウトした場合には、ステップS16およびS17を実行することなくステップS13へ進む。すなわち、本体装置20から使用許可信号を受信できなかった場合には、このICカードは、本体装置20の間でデータを送受できない。

【0027】なお、ステップS5において、指紋パターン格納部12に格納されている指紋パターンとパターン検出部2により検出された指紋パターンとが一致しないと判断した場合には、OK信号を出力することなくステップS14へジャンプし、その検出した指紋パターンをクリアした後に電源をオフにする。

【0028】図6は、第1の実施例における本体装置の処理のフローチャートである。この処理は、ICカード10が挿入されたことをトリガとして実行される。ステップS21およびS22では、ICカード10が挿入されたときから一定時間内にそのICカード10からOK

信号を受信したか否かを調べる。OK信号は、上述したように、指紋パターン格納部12に格納されている指紋パターンとパターン検出部2により検出された指紋パターンとが一致した場合にICカード10により出力される信号である。OK信号を受信した場合には、ステップS23へ進み、一方、受信できなかった場合には、ステップS25において挿入されたICカード10を排出する。

【0029】ステップS23では、ICカード10へ使用許可信号を送出する。この使用許可信号は、図5のステップS11およびS12において監視される信号であり、ICカード10は、この信号を受信すると、この本体装置とデータを授受できる状態になる。ステップS24では、ICカード10との間でデータを送受信する処理を実行する。なお、上述したOK信号は、ICカードの正規の使用者（所有者）とそのICカードに指紋を読み取らせた者とは一致しているか否かを表す情報なので、そのICカードの使用者を識別する情報はこのステップS24において受信する。したがって、もし、そのICカードの使用者を識別する情報が正規に登録されていなかった場合などには、OK信号を受信した場合であってもそのICカードに基づいた処理を拒絶することがある。また、この本体装置が、ICカード10とのデータの授受に際して不図示のホストコンピュータなどとの間でデータを授受する必要がある場合には、その処理はステップS24と並列に実行される。

【0030】このように、第1の実施例では、ICカードを使用する者が正規の使用者であるか否かをICカード自身が判断し、その判断結果を本体装置に通知する。そして、本体装置は、正規の使用者でない者の使用（すなわち、不正使用）であった場合には、そのICカードに基づく処理を禁止する。

第2の実施例

第2の実施例は、第1の実施例の構成に加え、指紋パターンの一致／不一致の判断が微妙な時に、使用者にパスワードを要求する機能を設けた構成である。なお、第2の実施例におけるICカードおよび本体装置の構成は、第1の実施例と同じであり、それぞれ図2および図3に示した通りである。

【0031】近年では、画像認識技術が進歩してきているが、一般に、パターンマッチング処理の精度は100パーセントではない。そして、この精度は、プロセッサの能力が低い場合や、短時間で処理しなければならない状況においては、低下するものと予想される。したがって、カードを使用する者が正規の使用者であるか否かの判断は、第1の実施例において述べたように、指紋パターンの類似度を数値化したその値が所定の閾値よりも大いにか否かに基づいて決定する方法が現実的である。ところが、この閾値の設定は難しく、一致／不一致の判断を甘くすれば不正使用を排除できない恐れがあり、反

対に、その判断を厳密にすれば、正規の使用者が使用しているにも関わらずその正規の使用者によるアクセスを拒絶してしまうことも起こりかねない。

【0032】そこで、第2の実施例では、ICカードは、指紋パターンの類似度を複数段階で評価し、ICカードに基づく処理を許可するか否かに際して、きめ細かい判断をできるようにした。具体的には、指紋パターンの類似度を、「非常に高い」、「比較的高い」および「低い」の3段階で評価して出力し、本体装置は、「類似度が非常に高い」を受信したときには、そのまま処理を許可するが、「類似度が比較的高い」を受信したときには、使用者にパスワードを要求する。

【0033】図7は、第2の実施例におけるICカードの処理のフローチャートである。この処理は、第1の実施例と同様に、ICカードの電源をオンにしたことをトリガとして実行される。なお、図7において、照合処理（ステップS7）、タイマ起動処理（ステップS7）、クリア処理（ステップS14）、電源オフ処理（ステップS15）は、第1の実施例と同じである。

【0034】ステップS31では、パターン検出部2により指紋パターンを検出する。この処理は、第1の実施例のステップS1～S3およびS8と同じである。続いて、ステップS4において、指紋パターン格納部12に格納されている指紋パターンとパターン検出部2により検出された指紋パターンとを照合し、その類似度を数値化する。

【0035】ステップS32では、ステップS4で得られた類似度が、「非常に高い」に属するか否かを調べる。類似度が非常に高ければ、ステップS33においてOK1信号を出力し、そうでなければ、ステップS34へ進む。ステップS34では、ステップS4で得られた類似度が、「比較的高い」に属するか否かを調べる。類似度が比較的高ければ、ステップS35においてOK2信号を出力する。OK1信号またはOK2信号を出力した場合には、ステップS7において、タイマ18を起動する。

【0036】ステップS36は、使用許可信号を監視する処理、および使用許可信号を受信した場合に本体装置との間でデータを送受信する処理である。これらの処理は、第1の実施例のステップS11、S12、S16およびS17と同じである。ステップS37では、OK1信号またはOK2信号をリセットする。即ち、OK1信号またはOK2信号の出力を停止する。なお、これらの信号をリセットする処理は、タイマ18のタイムアウトした場合、あるいは本体装置から使用許可信号を受信した場合に実行される。この後、ステップS14およびS15において、パターン検出部2により検出したパターンをクリアし、ICカードの電源をオフにする。

【0037】なお、ステップS4で得られた類似度が低いと判断した場合（ステップS32：N、かつステ

プS34:N0)には、正規の使用者でない者がこのICカードを使用しているものとみなし、OK1信号またはOK2信号のいずれも出力することなく、ステップS14へジャンプする。

【0038】図8は、第2の実施例における本体装置の処理のフローチャートである。この処理は、第1の実施例と同様に、ICカードが挿入されたことをトリガとして実行される。

【0039】ステップS41～S43は、挿入されたICカードから所定時間内にOK1信号またはOK2信号を受信したか否かを監視する処理である。OK1信号を受信した場合、すなわちICカードにおいて照合された2つの指紋パターンの類似度が非常に高い旨の通知を受けた場合には、そのICカードを使用している者が正規の使用者であるとみなし、ステップS23において使用許可信号を送出する。そして、ステップS24において、ICカードとの間でデータを送受信する処理を実行する。これらのステップS23およびS24は、第1の実施例における処理と同じである。

【0040】OK信号2を受信した場合、すなわちICカードにおいて照合された2つの指紋パターンの類似度が比較的高い旨の通知を受けた場合には、そのICカードを使用している者が正規の使用者である可能性が高いもののそうでない可能性もあるとみなし、ステップS44においてパスワードを要求する。続いて、ステップS45では、まず、その挿入されたICカードを識別する情報をそのICカードから読み取り、その識別情報に対して予め登録されているパスワードを抽出しておく。そして、上記要求に答えてカード使用者により入力されたパスワードとその予め登録されているパスワードとを照合する。ステップS46では、ステップS45における照合の結果を判断し、パスワードが一致していればステップS23へ進んで、使用許可信号を送出する処理、およびICカードとの間でデータを送受信する処理を実行し、一致していなければ、これらの処理をスキップしてステップS25へ進む。

【0041】所定時間内にOK1信号またはOK2信号のいずれも受信できなかった場合には、ICカードを使用している者が正規の使用者ではないとみなし、使用許可信号を送出することなくそのICカードを排出する。

【0042】このように、第2の実施例では、指紋パターンの照合結果のみではICカードを使用している者が正規の使用者であるのか否かを判断できない場合に、使用者にパスワードを入力させる構成を導入した。この結果、正しいパスワードを知らない不正使用者を確実に排除できると共に、正規の使用者が使用できないような状況は回避される。また、パスワードを併用するので、指紋パターンの照合の精度がそれほど高くなくてもICカードを使用する者が正規の使用者であるのか否かを判断できる。したがって、ICカード内に設けるCPUの性能は

それほど高くなくてもよく、ICカードの自体のコストアップを抑えられる。

第3の実施例

第3の実施例は、指紋パターンを照合する処理をICカードが挿入される本体装置において実行する構成である。

【0043】図9は、第3の実施例のICカードの構成図である。第3の実施例のICカードは、基本的には第1または第2の実施例と同じ構成であるが、指紋パターンを照合する処理を実行しないので、照合部16は設けられていない。

【0044】図10は、第3の実施例の本体装置の構成図である。第3の実施例の本体装置は、基本的には第1または第2の実施例と同じ構成であるが、指紋パターンを照合する処理を実行する。このため、CPU31がメモリ24に格納されているプログラムを実行することによって得られる機能の一部として照合部31が設けられている。

【0045】図11は、第3の実施例におけるICカードの処理のフローチャートである。この処理は、第1または第2の実施例と同様に、ICカードの電源をオンにしたことをトリガとして実行される。

【0046】ステップS51では、パターン検出部2により指紋パターンを検出する。この処理は、第1の実施例のステップS1～S3およびS8と同じである。続いて、ステップS52では、タイマ18を起動する。

【0047】ステップS53～S55は、タイマ18がタイムアウトする前に、このICカードが挿入された本体装置から指紋パターンの送信要求を受信したか否か、および使用許可信号を受信したか否かを調べる処理である。本体装置から指紋パターンの送信要求を受信した場合には、ステップS56において、指紋パターン格納部12に格納されている指紋パターンおよびパターン検出部2により検出した指紋パターンを本体装置へ送受する。また、使用許可信号を受信した場合には、ステップS57およびS58において、本体装置との間でデータを送受信する処理を実行する。この処理は、このICカードが本体装置と接続されている間は継続される。

【0048】本体装置から使用許可信号を受信することなくタイマ18がタイムアウトした場合、または本体装置との接続が終了した場合には、パターン検出部2により検出した検出パターンをステップS59においてクリアし、ステップS60においてこのICカードの電源をオフにする。

【0049】このように、第3の実施例のICカードは、本体装置からの要求に応じて予め格納してある指紋パターンおよび検出した指紋パターンを送出する。本体装置はそれらの指紋パターンに基づいて使用を許可するか否かを判断する。そして、ICカードは、本体装置から使用許可が与えられたときにのみ本体装置との間でデータの送受信が可能となる。

【0050】図12は、第3の実施例における本体装置の処理のフローチャートである。この処理は、第1または第2の実施例と同様に、ICカードが挿入されたことをトリガとして実行される。

【0051】ステップS61～S63は、挿入されたICカードに対して指紋パターンの送出を要求し、所定時間内にその要求に応じて指紋パターンを受信できるかどうかを判断する処理である。ICカードから指紋パターンを受信した場合にはステップS64へ進み、受信できなかった場合には、ステップS68においてそのICカードを排出する。

【0052】ステップS64では、ICカードから受信した2つの指紋パターン、即ち指紋パターン格納部12に格納されている指紋パターンおよびパターン検出部2により検出した指紋パターンを照合する。この処理は、たとえば、図4のステップS4の処理と同じであり、類似度を数値化する手順を含む。ステップS65は、ステップS64における照合処理の結果を参照し、上記2つの指紋が一致するのかが判断する。一致する場合には、ステップS66においてICカードに対して使用許可信号を送出し、ステップS67においてそのICカードとの間でデータの送受信処理を実行する。一方、上記2つの指紋が互いに一致しなかった場合は、ステップS66およびS67をスキップしてステップS68へ進んでICカードを排出する。

【0053】このように、第3の実施例の本体装置は、挿入されたICカードから予め格納してある指紋パターンおよび検出した指紋パターンを受信し、それらの指紋パターンが互いに一致した場合にのみICカードに使用許可を与える。

【0054】なお、第3の実施例においても、上述の第2の実施例と同様に、指紋パターンの照合とパスワードとを併用する構成としてもよい。このように、第3の実施例では、ICカードにおいて指紋パターンの照合処理を実行しないので、ICカードに設けるCPUは高い性能を持つ必要がない。したがって、ICカードの製造コストを低く抑えることができる。

【0055】なお、上記第1～第3の実施例では、各ICカードに1人の使用者の指紋パターンを予め格納しておく構成を示したが、本発明は、この形態に限定されるものではない。たとえば、家族や特定のグループの人間がICカードを共有できるようにしてもよい。この場

合、ICカードに予め複数人の指紋パターンを登録しておき、検出した指紋パターンとそれら複数の指紋パターンとを1つずつ照合してゆけばよい。

【0056】

【発明の効果】ICカードが正規の使用者により使用されているのか否かの判断を指紋パターンを用いて行うので、セキュリティが高い。このとき、カード使用者は、従来のようにパスワード等を覚えておく必要はなく、また、パスワード等の流出の恐れもない。さらに、ICカードを使用する際の操作も簡単である。

【図面の簡単な説明】

【図1】本実施形態のICカードの外観図である。

【図2】第1および第2の実施例のICカードの構成図である。

【図3】第1および第2の実施例の本体装置の構成図である。

【図4】第1の実施例のICカードの処理のフローチャート（その1）である。

【図5】第1の実施例のICカードの処理のフローチャート（その2）である。

【図6】第1の実施例の本体装置の処理のフローチャートである。

【図7】第2の実施例のICカードの処理のフローチャートである。

【図8】第2の実施例の本体装置の処理のフローチャートである。

【図9】第3の実施例のICカードの構成図である。

【図10】第3の実施例の本体装置の構成図である。

【図11】第3の実施例のICカードの処理のフローチャートである。

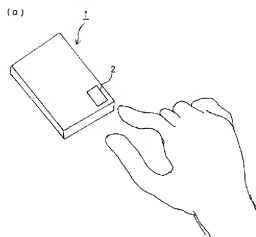
【図12】第3の実施例の本体装置の処理のフローチャートである。

【符号の説明】

1	ICカード
2	パターン検出部
11、13、24	メモリ
12	指紋パターン格納部
15、23	CPU
16、31	照合部
18	タイマ
21	カード挿入部
22	I/F部

【図 1】

本実施形態のICカードの外観図

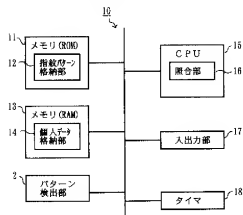


(b)



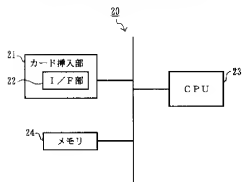
【図 2】

第1および第2の実施例のICカードの構成図



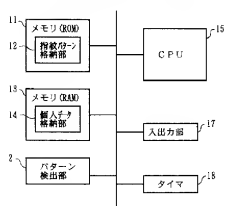
【図 3】

第1および第2の実施例の本体装置の構成図



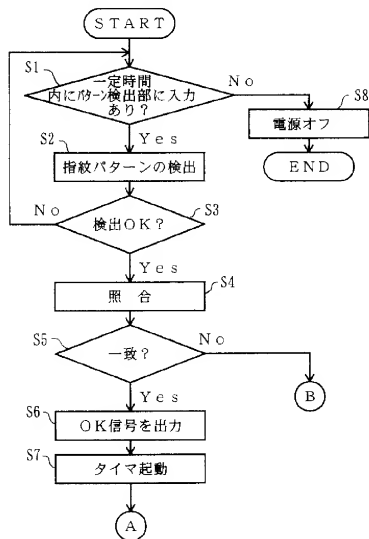
【図 9】

第3の実施例のICカードの構成図



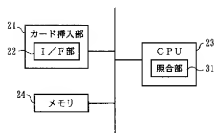
【図4】

第1の実施例のICカードの処理のフローチャート（その1）



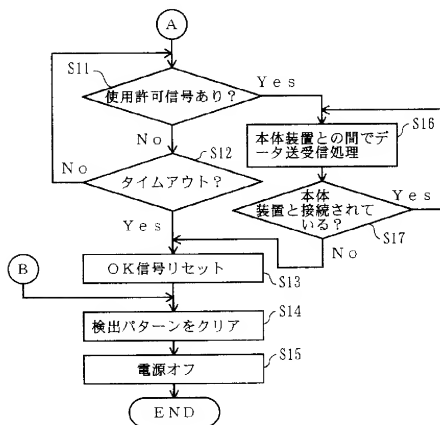
【図10】

第3の実施例の本体装置の構成図



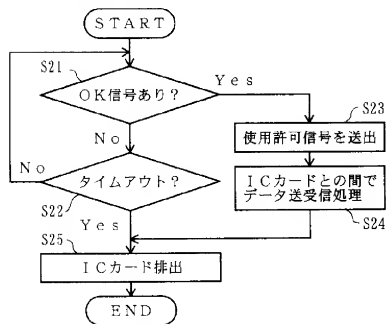
【図5】

第1の実施例のICカードの処理のフローチャート（その2）



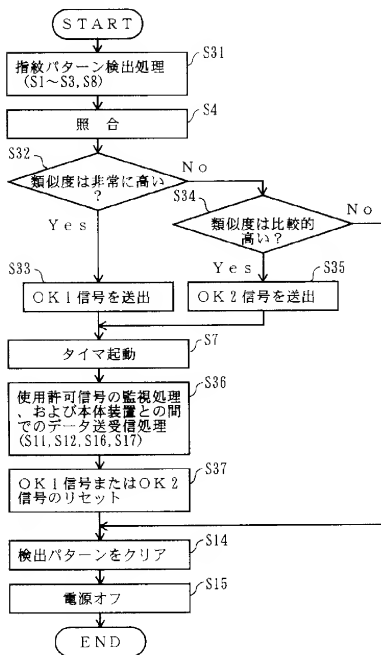
【図6】

第1の実施例の本体装置の処理のフローチャート



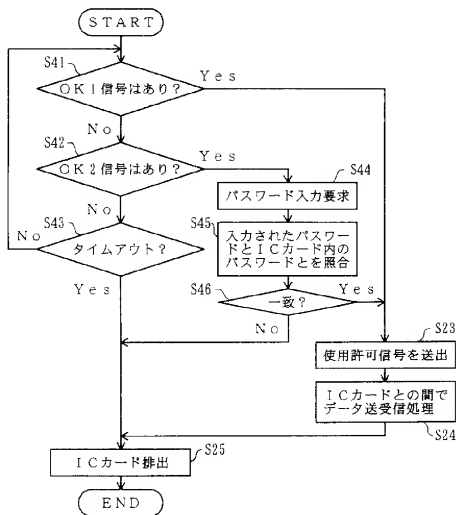
【図7】

第2の実施例のICカードの処理のフローチャート

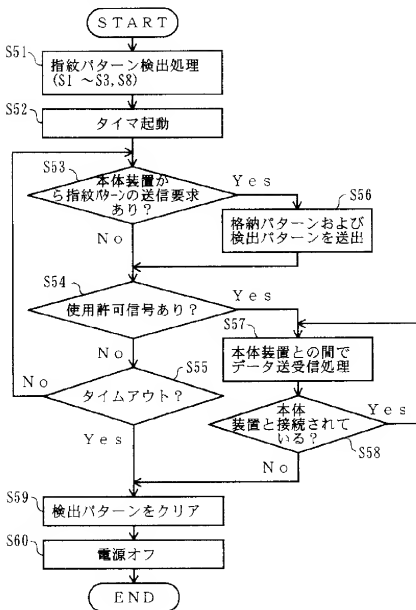


【図8】

第2の実施例の本体装置の処理のフローチャート



第3の実施例のICカードの処理のフローチャート



【図12】

第3の実施例の本体装置の処理のフローチャート

